**Ahmed Bouridane**



**Ahmed Bouridane** received an “Ingenieur d’Etat” degree in electronics from “Ecole Nationale Polytechnique” of Algiers (ENPA), Algeria, in 1982, an M.Phil. degree in electrical engineering (VLSI design for signal processing) from the University of Newcastle-Upon-Tyne, U.K., in 1988, and an Ph.D. degree in electrical engineering (computer vision) from the University of Nottingham, U.K., in 1992. From 1992 to 1994, he worked as a Research Developer in telesurveillance and access control applications. In 1994, he joined Queen’s University Belfast, Belfast, U.K., initially as Lecturer in computer architecture and image processing and later on he was promoted to Reader in Computer Science. He is now a full Professor in Image Engineering and Security and leads the Computational Intelligence and Visual Computing Group at Northumbria University at Newcastle (UK), and his research interests are in imaging for forensics and security, biometrics, homeland security, image/video watermarking, medical engineering, cryptography and mobile and visual computing. He has authored and co-authored more than 350 publications and two research books on imaging for forensics and security; and Biometric Security and privacy.

Prof. Bouridane is a Senior Member of IEEE.

**Title :** Artificial Intelligence: Risks and Benefits

**Summary:** Artificial Intelligence (AI) refers to the ability of a computer program/machine to think and learn like a human. AI applications already pervade many industries, bringing potential benefits that have been predicted to massively increase economic growth rate in a number of developed economies. However, the introduction of such innovative technology also brings new challenges. This seminar identifies some of the emerging risk issues around the growing implementation of AI and examines current and possible future implications of so-called "strong" AI, outlining potential benefits and areas of concern and their potential impact of AI in the security and defence industry.

For example, in security and defence applications, AI-powered software and machine (robots) can dramatically alter the digital security threat landscape. On one hand, it could help to reduce cyber risk by better detecting attacks, but on the other hand it could increase if malicious hackers are able to take control. AI could enable more serious incidents to occur by lowering the cost of devising cyber-attacks and enabling more targeted incidents. The same programming error or hacker attack could be replicated on numerous machines. For example, one machine could repeat the same erroneous activity several times, leading to an unforeseen accumulation of losses. It is already estimated that a major global cyber-attack has the potential to trigger massive losses. In addition, AI could also enable autonomous vehicles, such as drones, to be utilised as weapons. Such threats are often underestimated.

Existing AI applications are built around so-called "weak" AI agents, which exhibit cognitive abilities in specific areas, such as driving a car, solving a puzzle or recommending products/actions. With the first tangible benefits of "weak" AI applications already being deployed across many industries, expectations for AI technology are rising and more development investments are being allocated in order to anticipate the benefits of more human-like or "strong" AI in future. Its introduction especially with the current Deep Neural Network technology will most likely be unprecedentedly disruptive to current business models.

This seminar will first define and describe the concept of AI and a history of its development given. The operation of an AI system will then be given followed by a discussion of the dangers and benefits of the technology in light of the recent advances including the concept of Deep learning technology.